VirtualPatent

Enabling the Traceability of Ideas Shared Online Using Decentralized Trusted Timestamping

Corinna Breitinger, Bela Gipp

Department of Computer and Information Science
University of Konstanz, Germany
{corinna.breitinger, bela.gipp}@uni-konstanz.de

Abstract

Online discussion and sharing platforms have enabled ideas to be disseminated more quickly than ever before. However, there are many good reasons why individuals hesitate to share their ideas online. In academia, for instance, researchers may not want their contribution to be made public until after it has been published to ensure that they are appropriately credited for their work. As a consequence, novel ideas or creative work tend to only be shared within a small circle of trusted peers instead of with wider audiences online. This status quo prevents other experts on a specific topic from contributing to the discussion. In this paper, we present a proof-of-concept implementation of an online discussion and sharing platform that addresses this problem. The web-based application, coined VirtualPatent, automatically timestamps each post a user shares by creating a distributed timestamp on the blockchain of the cryptocurrency Bitcoin – a method for trusted-timestamp creation that we published in a previous paper. Unlike platform-managed timestamps, timestamps stored on the blockchain are persistent and cannot be tampered with. The system thus enables the author of a posting made online to retrospectively prove the exact time that the specific contribution was first put forth in a tamperproof manner – similar to a published paper, but with the simplicity of writing a post on a social media website.

Keywords: sharing platforms; social media, trusted timestamping; intellectual property; blockchain applications

In: M. Gäde/V. Trkulja/V. Petras (Eds.): Everything Changes, Everything Stays the Same? Understanding Information Spaces. Proceedings of the 15th International Symposium of Information Science (ISI 2017), Berlin, 13th—15th March 2017. Glückstadt: Verlag Werner Hülsbusch, pp. 89—95.

1 Introduction[1]

The volume of content shared online is growing at unprecedented rates. As of 2016, every 60 seconds: 347,000 tweets are published on Twitter, 66,000 photos and videos uploaded to Instagram,[2] and 400 hours of video content added to YouTube (James, 2015). Unlike physical media, digital contributions online are susceptible to widespread distribution and modification, with no reliable mechanism for tracking content back to its earliest point and time of origin. This volatility of Web resources demands standards to "assure us that information can be verified and traced to its source" (Snapper, 1999: 127). Today, commercial services, such as CopyScape[3] or Searchlight[4], offer to search the Web for unauthorized redistribution of ideas and creative content. However, no tamperproof mechanism has been integrated directly into a social media platform to enable content creators, such as authors, academics, artists, musicians, photographers, or innovators to prove priority for their work and ideas when shared online.

Existing social discussion and sharing platforms typically associate all user-uploaded media with a timestamp, however, such platform-generated timestamps share the same shortcomings: They are (a) not tamperproof, and (b) not persistent. Centrally managed media timestamps can be manipulated, e.g. by the platform operator or hacked by an external party. Even when no malice is involved, social sharing platforms can experience technical failures, or simply cease to exist, resulting in no guarantee for platform-managed media timestamps to be accessible indefinitely.

In this paper, we propose attaching a mark of traceability and permanence to user contributions online using trusted timestamping on the blockchain. We subsequently demonstrate the approach in a proof-of-concept web application.

---

1 This paper includes research performed in the scope of the first author's Master thesis (Breitinger, 2016).

2 https://www.instagram.com/press/

3 http://www.copyscape.com

4 http://www.searchlig.ht

2 Trusted timestamping of digital media

Decentralized Trusted Timestamping (DTT) using the blockchain is a recently introduced technical solution to solve the problem of securely verifying the time at which digital content existed in a certain state (Gipp, Meuschke & Gernandt, 2015). In this digital timestamping approach, the unique hash digest, e.g. SHA-256, generated from the given digital file is embedded as a transaction in a cryptocurrency's decentralized blockchain.[5] Due to the infrastructure of Bitcoin's blockchain (Nakamoto, 2008), it is computationally infeasible to manipulate transaction records, meaning timestamps are stored on a tamperproof and persistently verifiable medium.

While timestamping digital files is not new (Haber & Stornetta, 1991), DTT is an improvement upon the traditional digital timestamping (DTS) protocols that rely on a centralized third party to act as a Time Stamping Authority (TSA). Timestamping protocols include the RFC 3161 standard for trusted timestamps (Adams & Pinkas, 2001), or the ANSI ASC x9.95 Standard (ANSI, 2005). Unlike DTS, DTT does not require users to place trust in a TSA, which are typically commercial, and thus eliminates the risk of generated timestamps becoming invalid, e.g. if the TSA's private keys used for the public key encryption scheme were to become compromised.

Today, few content creators benefit from trusted timestamping to secure the time of existence of their contributions. We present an easy-to-use platform that implements DTT in the background to timestamp user-uploaded digital media, free of charge and with no added effort. We hypothesize that providing a method for securely verifying the date of existence of media shared online – independent of the distribution platform – is a key step toward (1) making the origin of ideas traceable and (2) increasing the user's incentive to share.

5 Space limitations prohibit us from discussing blockchain in more detail; for an overview of blockchain technology and its implications, please consult (Swan, 2015).

3 System design and implementation

The system is implemented as a *flask*[6] web application with a Python backend and a SQLite database. The application is hosted on Heroku as a demo and should be seen as a proof-of-concept[7]. We invite others to develop their own applications upon our idea, which is why the source code is available under an MIT license at: www.gipp.com/dtt. On the platform, users can create profiles and upload a variety of file formats. In a previous paper, we introduced a mobile application that focused exclusively on timestamping video files, specifically the video recorded by dashboard cameras (Gipp, Kosti & Breitinger, 2016). VirtualPatent calculates the unique hash for the uploaded file using *hashlib*'s SHA-256 function[8]. This hash is submitted for timestamping in Bitcoin's blockchain via OriginStamp's API.[9] Figure 1 shows the communication between the web application and the OriginStamp service to generate the timestamp on the blockchain. To avoid bloating the blockchain with unnecessary transactions, and to minimize transaction costs (to keep the timestamping service free of charge), OriginStamp collects all hashes received over a 24-hour period and generates one aggregate hash (SHA-256), see top right box in figure 1. From this aggregate hash, a new Bitcoin address is computed to which a one-time transaction of a Satoshi (0.00000001 Bitcoin) is sent. The transaction time at which the hash is embedded into the blockchain network becomes the timestamp of the file. Due to space limitations, please consult (Gipp et al., 2015) for the technical details on timestamp generation.

6 http://flask.pocoo.org/

7 The demo is accessible via: https://www.gipp.com/virtualpatent.

8 https://docs.python.org/3/library/hashlib.html

9 http://www.originstamp.org/developer

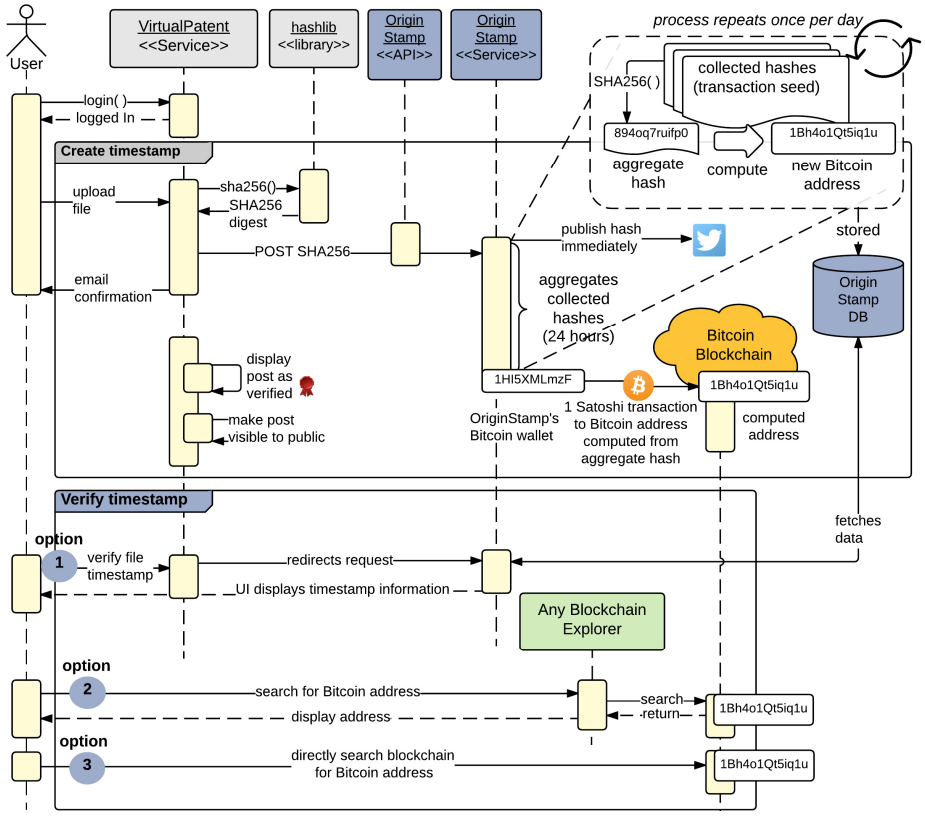

Fig. 1 Timestamp creation and verification process for files shared on VirtualPatent

Since the content is timestamped with a delay, users have the choice to keep their post private until the transaction has been confirmed in the blockchain network. To verify the timestamp of a file, the unique file hash and a 'verification link' are displayed with each post. The verification link currently redirects to OriginStamp's database of submitted timestamps, but could redirect to any blockchain explorer that provides users a GUI for verifying transactions in the blockchain network, see 'option 2' in figure 1. VirtualPatent additionally sends registered users an email confirmation once their file has been timestamped. The email includes the list of hashes used to generate the aggregate hash from which the Bitcoin address was computed. Sharing this data with the user guarantees that even if our platform or the OriginStamp service ceases to exist, users have a copy of all data required to verify that their file's hash was indeed embedded in a transaction on the blockchain.

The frontend of the VirtualPatent platform emphasizes ease of use and supports the actions that users expect of online discussion and sharing platforms, including profile creation and management, browsing posts, liking and sharing posts, commenting on posts, and following users. The system's functionality was inspired by the widely-used idea and knowledge exchanging platforms Quora and StackExchange.

4 Conclusion

Discussion and sharing platforms have enabled the barrier-free dissemination of creative work and ideas. However, no reliable method exists for tracing original ideas to their first time of existence online. We proposed the automatic and immutable timestamping of digital media shared online using trusted timestamping on the blockchain and presented VirtualPatent, a proof-of-concept platform. The timestamps that VirtualPatent creates for users' files are independent of the social sharing and discussion platform itself. Even if the platform were to cease to exist, the timestamps associated with the files can still be verified in the decentralized ledger that is the blockchain. This allows the user to prove the date of origin for their idea or contribution. Having an accessible and secure means to prove priority for an idea may encourage creatives to more openly share ideas and work online. In the future, we plan to integrate the approach demonstrated by VirtualPatent into other document management tools, such as Docear (Beel et al., 2011; Beel et al., 2014), to enable researchers to timestamp their ideas while writing their manuscript.

Acknowledgements

This research was partially funded by the Carl-Zeiss Foundation.

References

Adams, C., and D. Pinkas (2001): Internet X. 509 public key infrastructure time-stamp protocol (TSP).

American National Standards Institute (ANSI) (2005): X9 x9.95-2005 trusted time stamp management and security.

Beel, J., B. Gipp, S. Langer, and M. Genzmehr (2011): Docear: An Academic Literature Suite for Searching, Organizing and Creating Academic Literature. In: *Proceedings of the 11th ACM/IEEE Joint Conference on Digital Libraries (JCDL '11)*. ACM. http://doi.org/10.1145/1998076.1998188

Beel, J., S. Langer, B. Gipp, and A. Nuernberger (2014): The Architecture and Datasets of Docear's Research Paper Recommender System. In: *D-Lib Magazine – The Magazine of Digital Library Research*, 20 (11/12). http://www.dlib.org/dlib/november14/beel/11beel.html

Breitinger, C. (2016): *Using the Blockchain of Cryptocurrencies to Encourage Open Discussion and Sharing of Ideas*. MS Thesis, Linnaeus University.

Gipp, B., J. Kosti, and C. Breitinger (2016): Securing Video Integrity Using Decentralized Trusted Timestamping on the Blockchain. In: *Proceedings of the 10th Mediterranean Conference on Information Systems (MCIS)*, Paphos, Cyprus.

Gipp, B., N. Meuschke, and A. Gernandt (2015): Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. In: *Proceedings of the iConference 2015*. Newport Beach, California. http://ischools.org/the-iconference/

Haber, S., W.S. Stornetta (1991): How to Time-Stamp a Digital Document. In: *Advances in Cryptology – CRYPTO '90 Proceedings*, 3 (2), 99–111. http://doi.org/10.1007/BF00196791

James, J. (2015): Data Never Sleeps 3.0. https://www.domo.com/blog/data-never-sleeps-3-0/

Nakamoto, S. (2008): Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Snapper, J. W. (1999): On the Web, plagiarism matters more than copyright piracy. In: *Ethics and Information Technology*, 1 (2), 127–135.

Swan, M. (2015): *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc.